Monitoring Strategies for Detection of Insider Threats

Dawn M. Cappelli

Michael P. Hanley

CERT Insider Threat Center

http://www.cert.org/insider_threat/

Notices

Agenda

Introduction

Development of Insider Threat Controls *

Detection Strategies

Questions

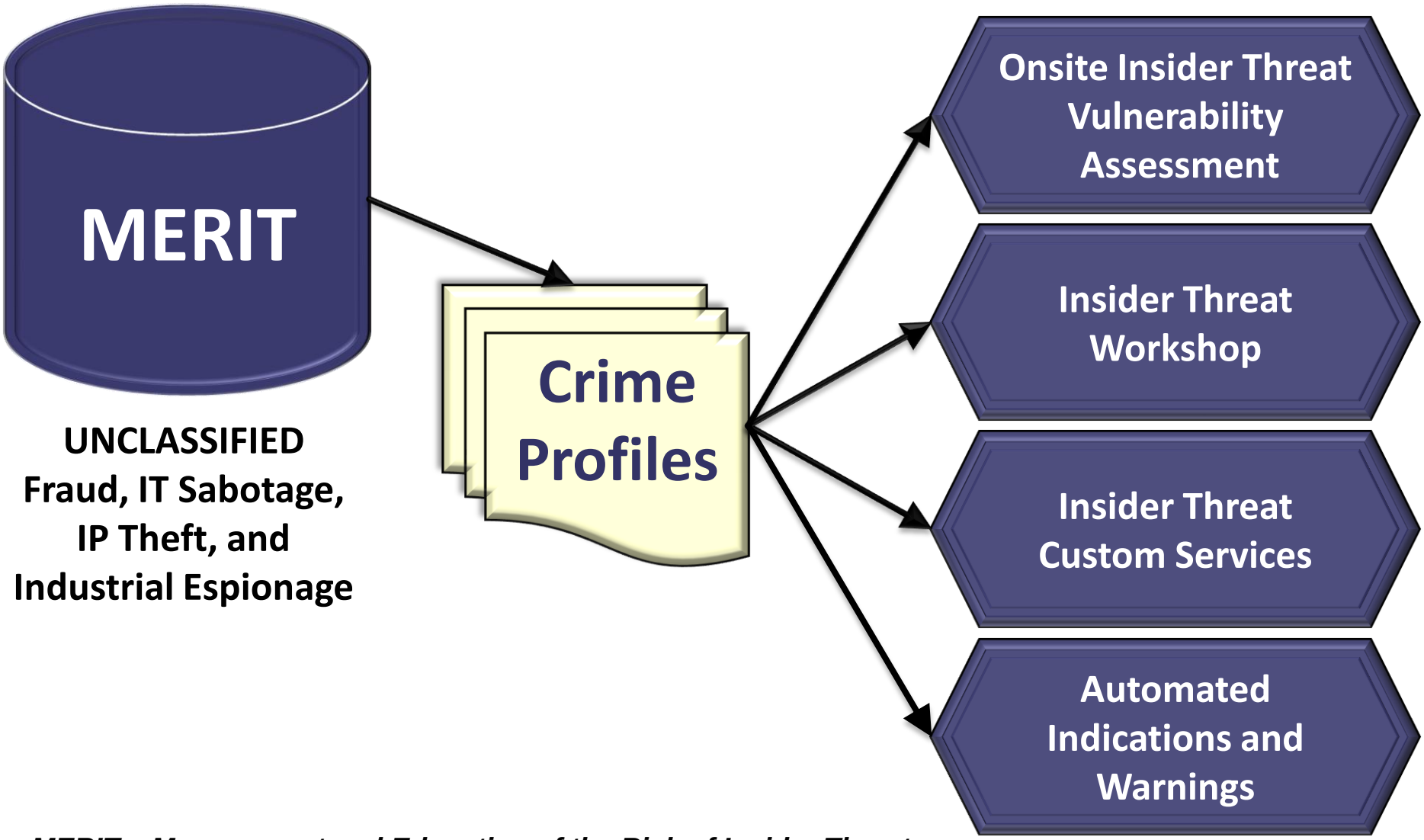
*This work is currently funded by DHS Federal Network Security

Who is a Malicious Insider?

Current or former employee, contractor, or other business partner who

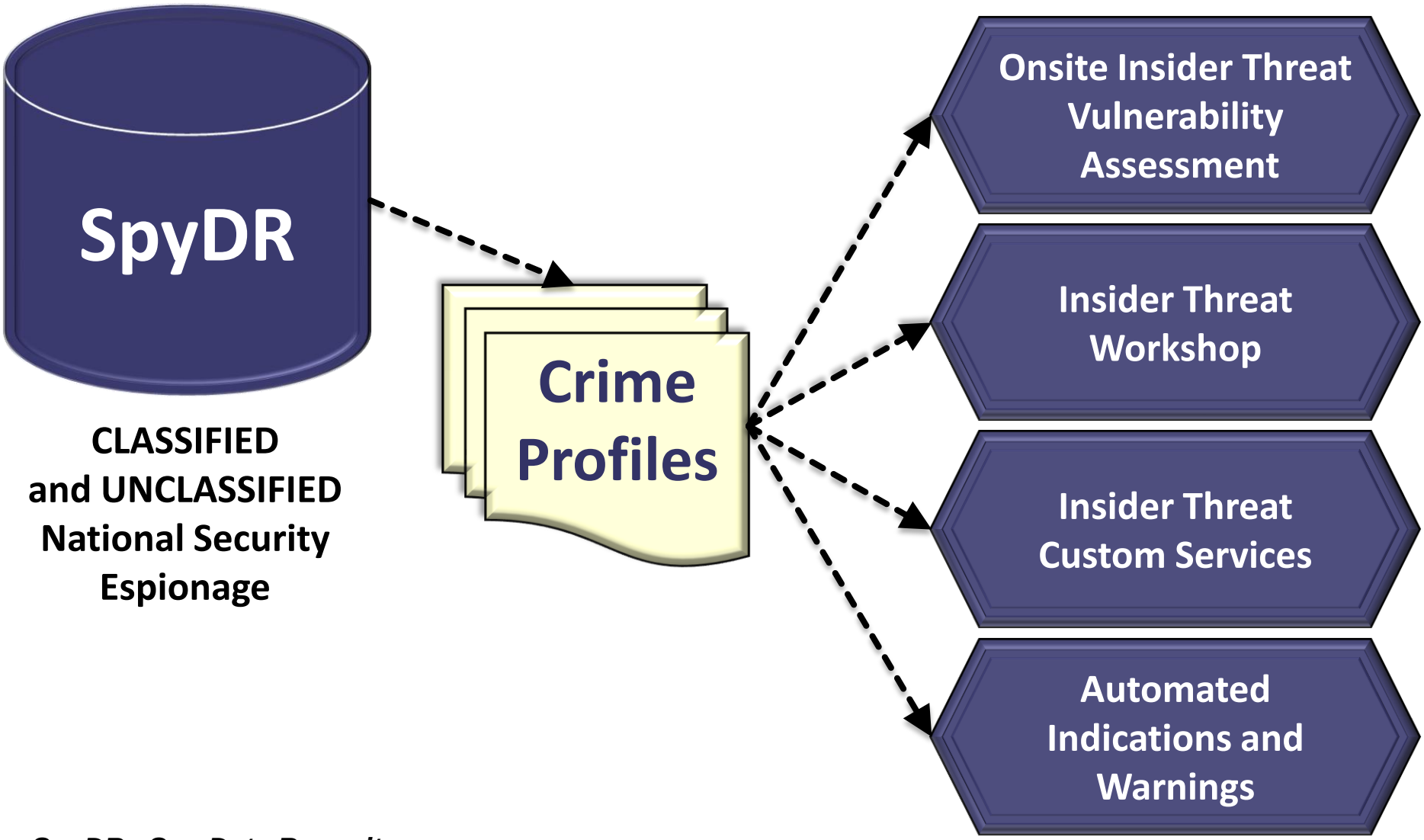
- *has or had authorized access to an organization's network, system or data and*
- *intentionally exceeded or misused that access in a manner that*
- *negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.*

CERT's Insider Threat Portfolio



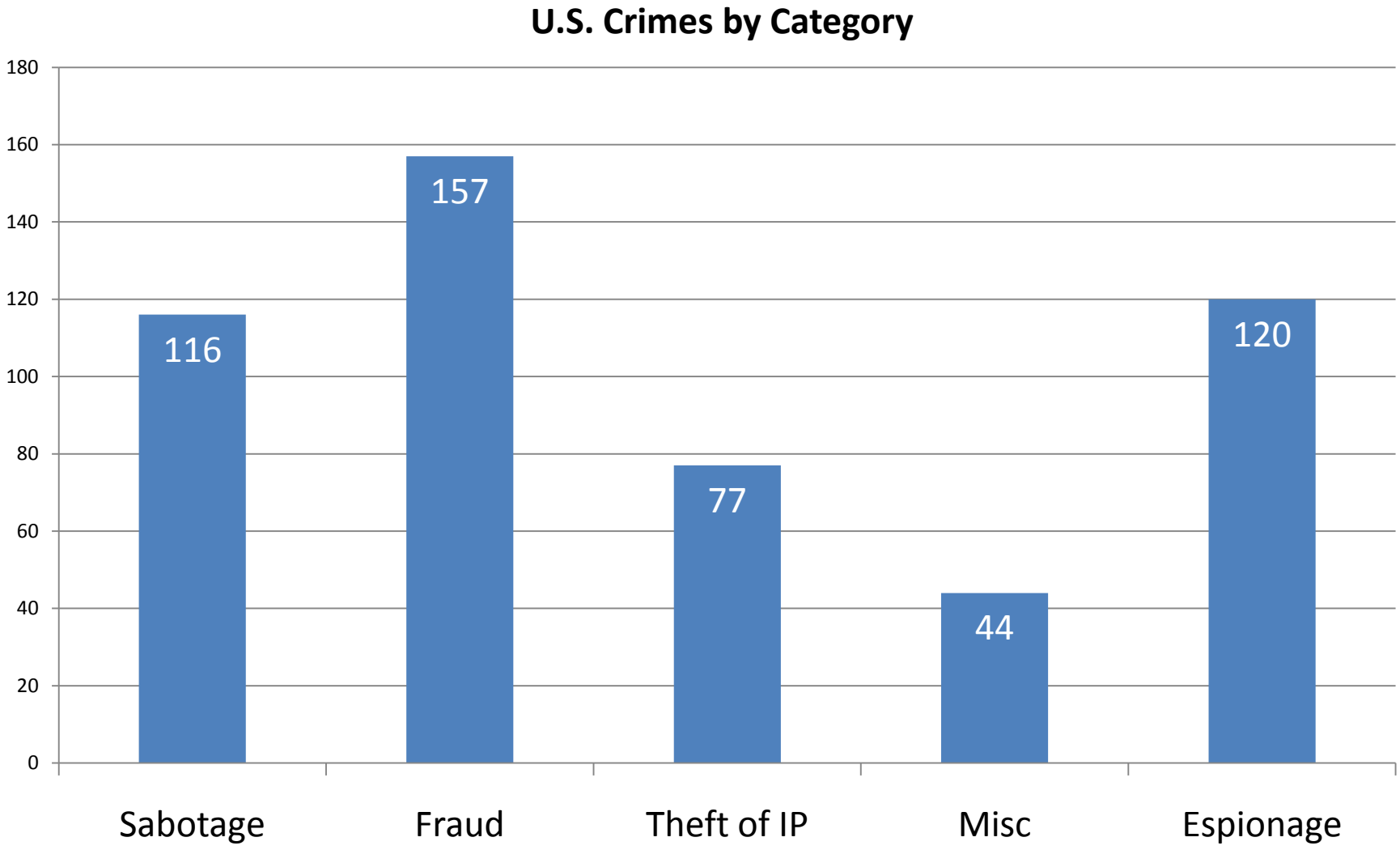
MERIT – Management and Education of the Risk of Insider Threat

CERT's Insider Threat Portfolio



SpyDR– Spy Data Repository

CERT's Insider Threat Case Database



Current Body of Work

Cases
Assessments
Metrics
Lit Reviews

Incident Response
Forensic Investigations (internal & external attacks)
Standards

Controls
Open source solutions
Optimized configurations for commercial technology
Risk scoring algorithms
New functional requirements

Insider threat risk management process
Workshops
Senior Executive Workshops
Demos
VTE Modules
Exercises

Development of Insider Threat Controls

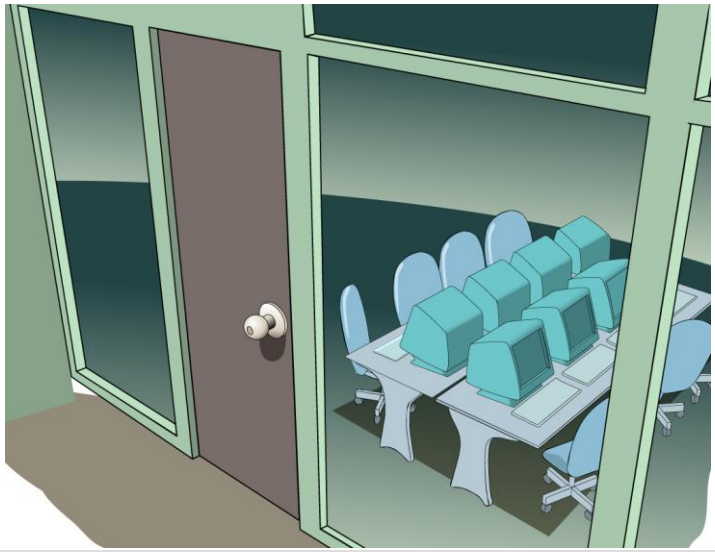
Insider Threat Control Development

- Use insider threat database to “deep dive” into cases to understand how insiders exploit organization systems
  - Includes ~4000 identified issues of concern, vulnerabilities, and observed exploits derived from 400+ catalogued cases
- From this, create formal controls/recommendations to defend against these types of exploits, including:
  - Examples of firewall or IDS rules/signatures
  - Suggested system logging/auditing controls
  - Change control management
- Controls will be tested in the CERT Insider Threat Lab for feasibility, compatibility with various platforms and applications
- Test for effectiveness through recreating insider exploits in the lab environment

CERT Insider Threat Lab - History

Initially funded by Carnegie Mellon's CyLab and the DOD

- Stood up equipment
- Conducted analysis of tools designed to combat insider threat
- Produced several demonstrations of actual insider attacks
  - ***Demo 1****:* Insider data exfiltration via unauthorized chat
  - ***Demo 2****:* Use of netflow to locate insiders removing large volumes of data from the network
  - ***Demo 3****:* Principles for finding insiders who use e-mail as their data exfiltration method
- Whitepaper examining the current tool space associated with insider threat defense and data loss prevention



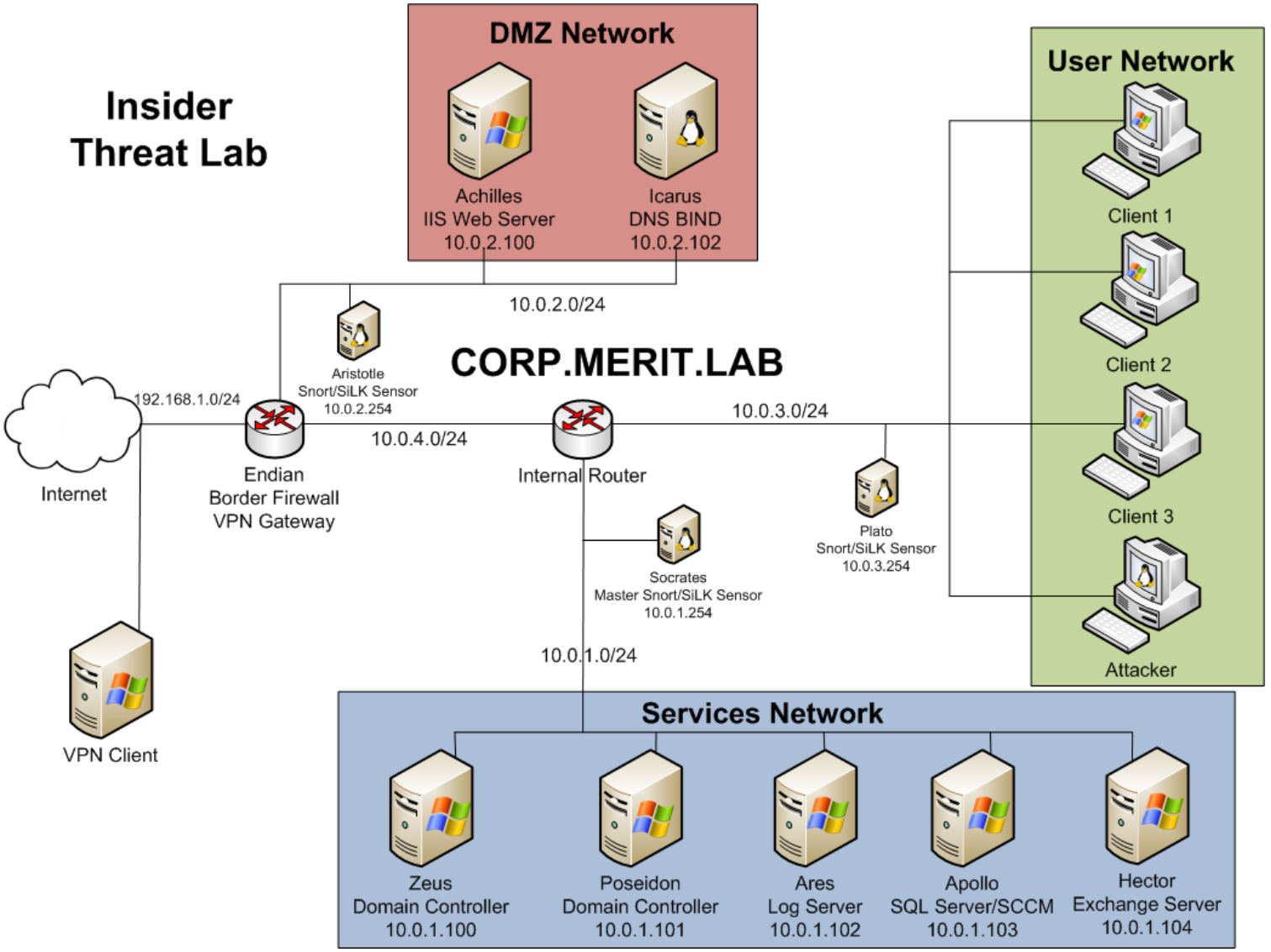
CERT Insider Threat Lab - Current

Funded by DHS Federal Network Security

Focus: Insider Threat Controls

- Development of new technical controls designed to enhance the security posture of federal systems against insider attacks.
- Controls can be deployed and used in federal network security operations with ease through the use of implementation guidelines.
- Controls will be included in Insider Threat Assessment

Current Lab Demonstration Network



Detection Strategies

IT Sabotage


DAN
DAN
SLAM!
Attach File(s)
Do you want
to attach DAN_BACKDOOR.EXE?
YES
NO

High Level View of Insider IT Sabotage

	IT Sabotage
Current or former employee?	Former
Type of position	Technical (e.g. sys admins or DBAs)
Target	Network, systems, or data
Access used	Unauthorized
When	Outside normal working hours
Where	Remote access
Recruited by outsiders	None
Collusion	None

Detection of Insider IT Sabotage

Problems:

- Privileged users
  - Can insert malicious code just about anywhere and it is not anomalous activity
  - Have the ability to override system controls without detection
  - Have special knowledge of vulnerabilities in IT systems
  - Have used hack tools against their organization
- Unauthorized accounts are a common method for gaining access following termination
- Account creation is not anomalous activity for many privileged users
- Account audits are not streamlined and can be very resource intensive
- Information overload: Good instrumentation is helpful, but you can't realistically monitor everything everyone does online

Detection of Insider IT Sabotage

Solution Strategies:

- Learn from the MERIT models and from past cases
- Implement continuous logging and centralized, secure log server
- Detect and investigate changes that should occur infrequently, e.g.
  - Changes to operating system files, scripts, and executables
  - Changes to stable production systems
  - Services killed on host
- Audit individual actions in logs for privileged accounts
  - Especially for insiders who are “on the HR radar”
- Scan workstations regularly for potentially offensive tools
- Audit access to backup information and results of backup and recovery tests carefully – this is your last line of defense!

Detection of Insider IT Sabotage

Solution Strategies (cont'd):

- Configure Intrusion Detection systems and proxies to alert on suspicious outbound traffic
- Audit failed physical access attempts
- Alert on creation of new accounts and frequently validate existing accounts
- Control shared accounts

Fraud

High Level View of Insider Fraud

	IT Sabotage	Fraud
Current or former employee?	Former	Current
Type of position	Technical (e.g. sys admins or DBAs)	Non-technical, low-level positions with access to confidential or sensitive information (e.g. data entry, customer service)
Gender	Male	Fairly equally split between male and female

High Level View of Insider Fraud

	IT Sabotage	Fraud
Target	Network, systems, or data	PII or Customer Information
Access used	Unauthorized	Authorized
When	Outside normal working hours	During normal working hours
Where	Remote access	At work
Recruited by outsiders	None	½ recruited for theft; less than 1/3 recruited for mod
Collusion	None	Mod: almost ½ colluded with another insider Theft: 2/3 colluded with outsiders

Detection of Insider Fraud

Problems:

- Authorized users have added, modified, or deleted data in databases to commit fraud against the organization
- Collusion between employees occurred in approximately 50% of the cases, possibly to overcome separation of duties

Solution Strategies:

- Auditing database transactions may help detect unauthorized access and modification of data
- Auditing data changes for all tables in a database is not practical and may degrade performance
- Monitor access and data modifications on critical tables, such as tables containing PII or customer information
- Audit either successful or unsuccessful data access / modification attempts or both

Theft of Intellectual Property

High Level View of Insider Theft of IP

	IT Sabotage	Fraud	Theft of Intellectual Property
Current or former employee?	Former	Current	Current, but most within 30 days of announcing resignation
Type of position	Technical (e.g. sys admins or DBAs)	Non-technical, low-level positions with access to confidential or sensitive information (e.g. data entry, customer service)	Technical (71%) - scientists, programmers, engineers Sales (29%)
Gender	Male	Fairly equally split between male and female	Male

High Level View of Insider Theft of IP

	IT Sabotage	Fraud	Theft of Intellectual Property
Target	Network, systems, or data	PII or Customer Information	IP (trade secrets) – 71% Customer Info – 33%
Access used	Unauthorized	Authorized	Authorized
When	Outside normal working hours	During normal working hours	During normal working hours
Where	Remote access	At work	At work
Recruited by outsiders	None	½ recruited for theft; less than 1/3 recruited for mod	Less than 1/4
Collusion	None	Mod: almost ½ colluded with another insider Theft: 2/3 colluded with outsiders	Almost ½ colluded with at least one insider; ½ acted alone

Theft of IP: Detailed Analysis

"The CERT Insider Threat Lab: Analysis of Technical Methods Used in Insider Theft of IP and Countermeasures" (August 2010)

Deep technical examination of 50 cases involving theft of Intellectual Property (IP)

- Primary methods of theft/exploitation by insiders in each crime
- Types of assets targeted by insiders
- Methods of data exfiltration
  - Broken out by networked exfiltration methods and physical methods
- Insider attempts to conceal their actions (if any)
- Potential mitigation strategies (including analysis of DLP tools)
- Analysis of findings in concert with conclusions from "Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model" (Moore, et. al. 2009)

Theft of IP: Detailed Analysis

Findings:

- Most (54%) data exfiltration events we studied occur over the network and could be observed through proper network instrumentation.
- Of data exfiltration events involving the network, most occur though e-mail. Fortunately, all but one of the DLP tools studied supported some form of e-mail monitoring.
  - Most of this mail traffic goes directly to a competitor's domain or to a personal mail account. Consider queries based on mail destination.
- Most cases involved no effort to conceal the insider's actions from the organization
- Only half of the tools can detect and block sensitive print jobs.
- 56% of the tools studied support tracking data movement within an enclave network.
- DLP tools appear to be maturing, but there are still serious gap areas that require careful configuration and complementary tools

Theft of IP for Foreign Governments or Organizations

"Spotlight On: Insider Theft of Intellectual Property inside the U.S. Involving Foreign Governments or Organizations"* (June 2009)

Important findings:

- Twenty five percent of the insider theft of IP cases in the CERT database were for the benefit of a foreign government or organization.
- All of these cases involved espionage "rings" of insiders and/or outsiders.
- It is much more difficult, if not impossible, to recover IP once it leaves the U.S.

* http://www.cert.org/archive/pdf/CyLabForeignTheftIP.pdf

Detection of Insider Theft of IP

Problems:

- Massive volume of data makes monitoring and alerting difficult
- Difficult to baseline normal behavior and configure tools to identify abnormal behavior
- Insiders tend to steal the same data they access in the course of the normal workday
- Organizations may not detect unauthorized devices connected to their networks
  - Peripherals, e.g. keyloggers, removable media, backup systems, modems
  - Network devices, e.g. rogue laptops, access points, mobile devices
- It can be difficult to distinguish between legitimate and illegitimate use of removable media
- Laptops are a common means of intentional data exfiltration

Detection of Insider Theft of IP

Solution Strategies:

- Learn from the MERIT models and from past cases
- Log, monitor, and audit system logs for queries, downloads, print jobs, email messages containing unusually large amounts of data, PII, and sensitive IP
- Alert on emails to competitors, foreign locations, or personal email accounts
- Monitor network data for abnormally large file transfers, long connections, odd ports, illegal source/destination IP addresses, …
  - Baseline first to facilitate incident response later!

Detection of Insider Theft of IP

Solution Strategies:

- Audit logs for activity of resigning or terminating employees
  - Log all downloads to removable media
  - Alert when critical information is downloaded to removable media, e.g. intellectual property, customer information, PII
  - Log and alert on unidentified device/peripheral attachment
  - Consider prohibiting the use of personal devices for work-related activities
- Implement targeted monitoring of prior online activity of individuals who are "on the way out"
- Log, monitor, and audit for remote access from IP addresses from outside the U.S., from competitors' networks, and from terminating or terminated employees

Demonstration

Tracking mail flow to competitors/foreign entities with Splunk

- Ties closely back to CERT's theft of IP model by incorporating several principles (theft within 30 days of resignation, theft using e-mail, etc.) from a single case involving e-mailing confidential information to a competitor.
- Demonstrates how to use centralized logging (with Splunk) to automatically report on volume/destination of e-mail traffic for employees who have recently left the organization. Presents original and useful Splunk queries that can be easily put into operation by an organization.

Key Points to Remember

- Even on a well-instrumented network, there are still other limiting factors
- Index critical IP, focus your efforts on protecting these assets
- When an employee with privileged information is leaving the organization, be aware of their information access and use of communication channels
- Have a clearly defined policy for enterprise monitoring and acceptable use. Institutionalize this policy!
- Once your IP has left the network, you no longer have control over it’s distribution/confidentiality.

Final Thoughts

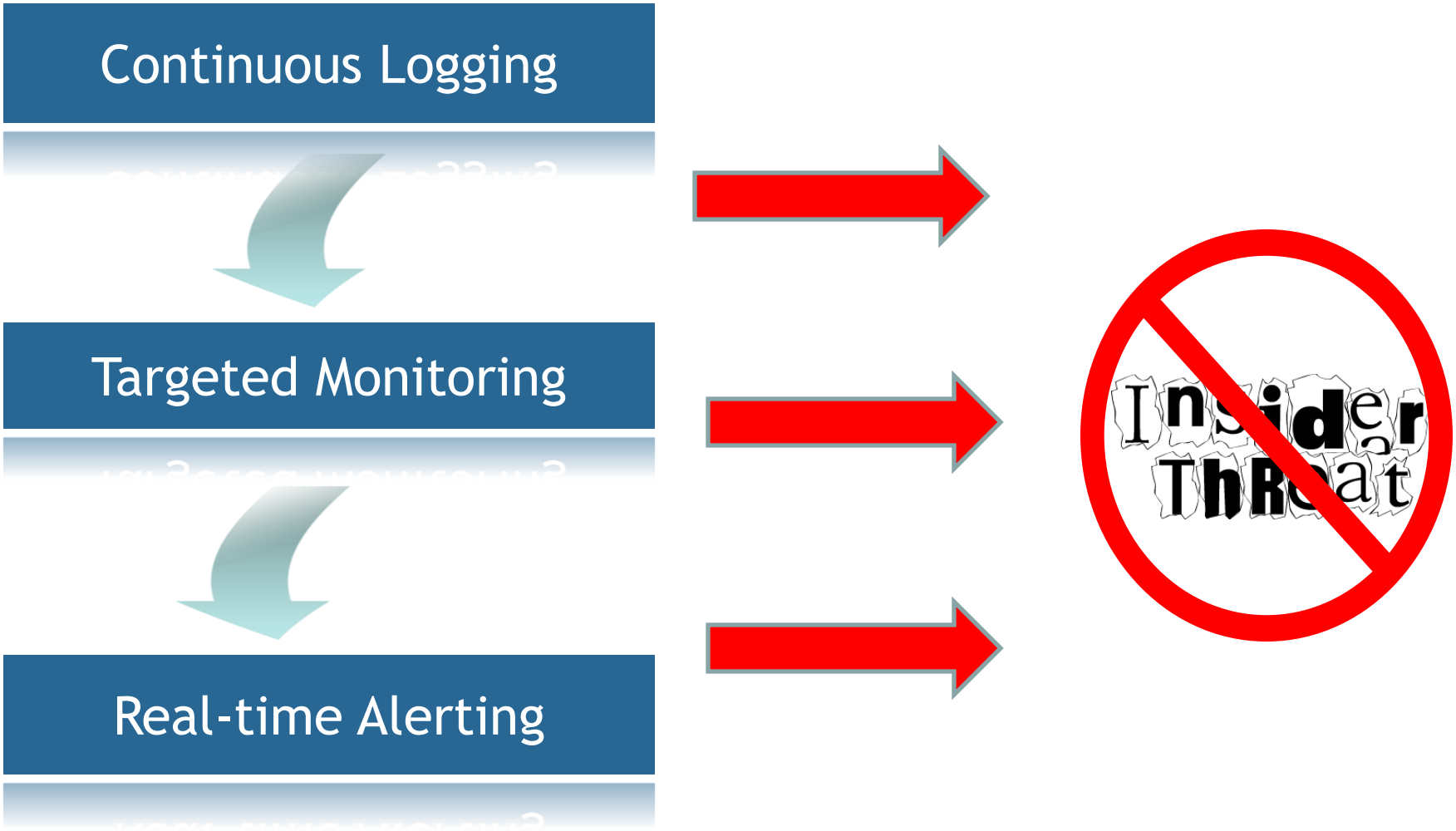
Caveats:

- We only have data on criminals
  - Our findings / recommendations could result in a high false positive rate
- These monitoring techniques are not a guarantee
  - In the event of a missed insider attack, these methods will be tremendously beneficial for incident response and forensic analysis teams
- Consider legal, privacy, and policy issues before implementing any employee monitoring program

Food for thought:

- Which of the monitoring techniques we've presented might also be effective in detecting external intruders if they manage to gain access?
- Could these controls be effective against both insiders and outsiders?

Summary


Continuous Logging
Targeted Monitoring
Real-time Alerting
Insider Threat

Points of Contact

Technical Manager, Threat and Incident Management
Dawn M. Cappelli
CERT Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-9136 – Phone
dmc@cert.org – Email

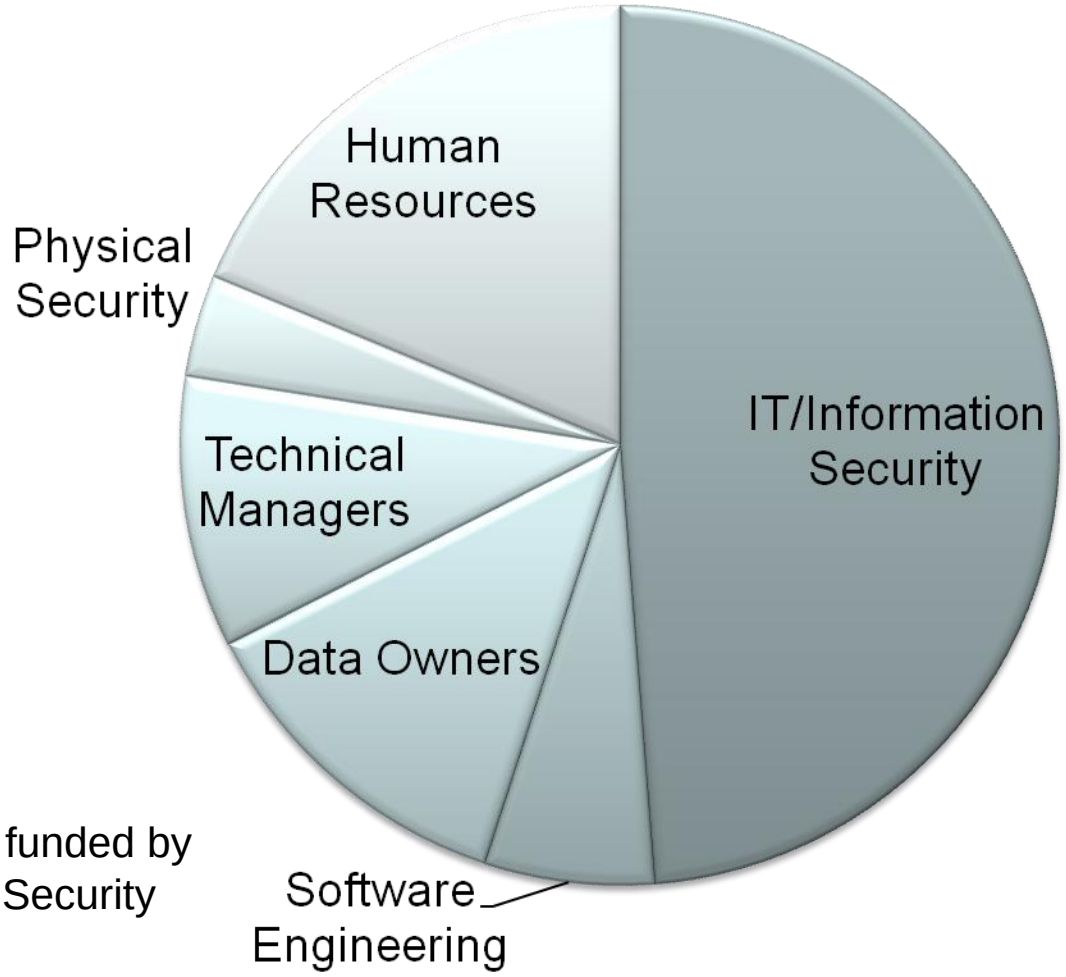
Michael P. Hanley
Lead, Insider Threat Solutions
CERT Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-8145 – Phone
mhanley@cert.org - Email

http://www.cert.org/insider_threat/

CERT Insider Threat Vulnerability Assessment

Addresses all types of vulnerabilities exploited in the cases we have studied

- Technical
- Psychological
- Process
- Policy



*This work is currently funded by DHS Federal Network Security